**Cybersecurity in CS Degrees**

*Cybersecurity will become an integral part of computing science education in the UK thanks to a coordinated approach from the BCS, the Council for Professors and Heads of Computing, (ISC)² and the Office of Cyber Security and Information Assurance within the Cabinet Office.*

## 1.0 The Need to Develop Protection Skills Against Cyber Threats

It is recognised that there is a lack of Cybersecurity skills in Computing Science degrees, yet Cybersecurity must be addressed in the design, development and operation of any IT system. This need is acknowledged by Objective 4 of the UK's Cyber Security Strategy: "to have the cross-cutting knowledge, skills and capability [needed to] underpin all our Cybersecurity objectives". Fulfilling Objective 4 addresses a severe skills shortage by widening the opportunity of a Cybersecurity career to more people and ensuring that everyone involved in creating the digital economy – especially the technology underpinning it – understand the threats, vulnerabilities and mitigations that need to be managed.

Embedding Cybersecurity skills into our Computing Science degrees will ensure that the UK leads the world in this key area. According to a recent CloudPassage report, just one of the 36 top ranked US College and University computing science programmes require students to take Cybersecurity classes and three of the top ten do not even offer classes on Cybersecurity. A recent SANS survey found that heads of computer science departments were typically disdainful of the need to ensure that students are aware of Cybersecurity issues, saying employers should do that kind of "training". Mary Davison, Oracle's CSO, found that Universities were generally unresponsive to requests that students studying programming learned how to secure their code. Matthew Hancock, Minister for the Cabinet Office said, "The UK has a world-class Cybersecurity sector, but we can only continue in this vein if we have the highly skilled workforce we need to thrive."

News coverage has the potential to embarrass the IT and academic professions, as many of the stories highlight errors in design, development and management of IT that have led to vulnerabilities that can be exploited. It's worth remembering that many of the exploits were well known, with well-known mitigation. This could be considered as a professional failing, as we are not adhering to a core principle of the BCS Code of Conduct to ensure that the public is protected when we take actions and make decisions in designing, deploying and managing systems.

Universities in the UK are graduating students on courses with a significant amount of ethical hacking, generating many graduates who are able to target and abuse systems, yet many Computing Science graduates do not understand how and why Cybersecurity and resilience are just as, if not more, important. The Council of Professors and Heads of Computing (CPHC) and (ISC)² suggest that exposure to more Cyber and information security concepts at the undergraduate level could help stem the flow of vulnerabilities we see in IT. However, it must be recognised that to have any profound impact the effort must be collaborative between industry, professional bodies and academia.

## 2.0 Big Tent Approach

In 2013, an initiative was set up by (ISC)², CPHC and the Cabinet Office to examine embedding Cybersecurity into undergraduate degrees. Three workshops in 2013 and 2014 defined the principles of Cybersecurity education and developed a framework for embedding these principles in UK Computing Science curricula. Attendees included industry, professional bodies, UK government departments and more than 30 Universities that offer undergraduate Computing Science degrees from the newest post-92 Universities to the Russell Group. Significantly, the BCS agreed to adopt the outputs into their accreditation

criteria during the workshops, the first time that Cybersecurity has been explicitly referenced within accreditation criteria for computing and IT-related degrees.

Bill Mitchell, Director of Education at the BCS, explained the reason for their involvement: “As an Institute we are already heavily involved in tackling the skills gap in this field; from developing the profession through to ensuring that standards are met. This latest initiative means that all computing-related degrees accredited by the BCS will now include information security learning elements”.

The final workshop resulted in the production of reference guidelines (“Cybersecurity Principles and Learning Outcomes”) that established a baseline of common knowledge, example learning outcome domains for Cybersecurity within the Computing Science courses and guidance on embedding the concepts. This ground-breaking effort means that, for the first time, UK Universities will benefit from specific guidance for embedding and enhancing relevant Cybersecurity principles, concepts and learning outcomes within their undergraduate curricula.

“This marks a significant shift in the teaching of security in higher education; Cybersecurity is now recognised as integral to every relevant computing discipline from computer game development to network engineering,” said Carsten Maple, Professor of Cyber Systems Engineering at Warwick University and Vice chair of the Council of Professors and Heads of Computing.

**3.0 Cybersecurity in Computing Science Guidelines**
The reference guidelines details five essential areas of Cybersecurity:

1. Information and risk: models including confidentiality, integrity and availability; concepts such as probability, consequence, harm, risk identification, assessment and mitigation; and the relationship between information and system risk.
2. Threats and attacks: threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities.
3. Cybersecurity architecture and operations: physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance.
4. Secure systems and products: the concepts of design, defensive programming and testing and their application to build robust, resilient systems that are fit for purpose.
5. Cybersecurity management: understanding the personal, organisational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how Cybersecurity is implemented.

By implementing the guidelines, over 20,000 computer science graduates a year across 100 UK Universities will be taught these five areas, significantly enhancing the UK’s capacity for filling the aforementioned skills shortage. Adrian Davis, Managing Director of (ISC)² EMEA explains that “including Cybersecurity in undergraduate education positions the UK as a world leader, provides a significant number of cyber-competent, well-educated people entering the jobs market generally, and highlights Cybersecurity career opportunities.”

**4.0 Taking it to the Masses!**
After the guidelines were published, a workshop roadshow was hosted by the Universities of Edinburgh Napier, Portsmouth, Lancaster, Hertfordshire, Cardiff, Royal Holloway, Newcastle and Warwick. These workshops, which presented the guidelines and the reasons for embedding Cybersecurity in the curriculum of Computing Science degrees, had 102 attendees from the academic Computing Science community representing 60 UK

Universities. The impact on accreditation and associated processes was considered and case studies from the Universities of Sunderland and Portsmouth, highlighting two different approaches to implementing the guidelines, were presented.

“The discussions were positive and constructive, providing an excellent forum to consider the opportunities and challenges, while identifying a range of good practices to inform next steps,” describes Alastair Irons, Professor of Computer Science, University of Sunderland and chair of the BCS Accreditation Committee, “Cybersecurity is now a key component of the BCS accreditation criteria, reflecting the importance placed on Cybersecurity and the expectation that all computing graduates should have knowledge and skills in Cybersecurity as they move towards Chartered status."

**5.0 Next Steps...**

A majority of representatives at the workshop roadshow were supporters of the need to embed Cybersecurity in the Computing Science curriculum. The next step is to widen and deepen support for this embedding process, by creating a community to share best practice, overcome implementation barriers and provide materials and guidance for those who need it, such as a resource library that is full of example pedagogic interventions that can be adapted for different scenarios within each institution. “There are many Universities that are producing innovative examples that engage students and demonstrate the need for Cybersecurity. I am excited by what could be achieved when this community is enabled to share and develop ideas,” said Dr. Nick Savage, Head of the School of Computing at the University of Portsmouth.

Cybersecurity is not the preserve of IT: it affects us all. Our next objective is to explore the integration of Cybersecurity into the teaching offered by Business and Management schools. Working with these schools and using the approach outlined here, we could create a second corpus of cyber-competent, well-educated people entering the workforce who understand Cybersecurity and its effects on organisations.

The full University guidelines can be found here: http://cert.isc2.org/isc2-cphc-whitepaper/